novática
Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI es miembro fundador de **CEPIS** *(Council of European Professional Informatics Societies)* y es representante de España en **IFIP** *(International Federation for Information Processing);* tiene un acuerdo de colaboración con **ACM** *(Association for Computing Machinery),* así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2**, **ASTIC**, **RITSI** e **Hispalinux**, junto a la que participa en **ProInnova**.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn. 963740173 <novatica_prod@ati.es>
Administración y Redacción ATI Cataluña
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235, fax 934127713 <secregen@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia<secregal@ati.es>
Suscripción y Ventas <http://www.ati.es/novatica/interes.html>, ATI Cataluña, ATI Madrid
Publicidad Padilla 66, 3º, dcha., 28006 Madrid.
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Imprenta: Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Gaia y los Titanes - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

sumario

Nº 218, julio-agosto 2012, año XXXVIII

Tema del próximo número: "Redes sociales y multicanalidad"

Mathias Vermeulen
Instituto Universitario Europeo de Florencia (Italia)

<mathias.vermeulen@gmail.com>

El secreto se impone a la ubicación: Estableciendo la gravedad de las injerencias en la privacidad que plantean las tecnologías de vigilancia

Traducción: Josep Moya Pérez (Grupo de Trabajo de Lengua e Informàtica de ATI)

Resumen: *Desde el 11 de septiembre del 2001, el uso de las tecnologías de detección ha sido visto cada vez más como un instrumento fundamental para combatir el terrorismo. La utilización y la implementación de estas herramientas a menudo no suponen una intromisión en el derecho a la privacidad, incluso con los medios que se usan en lugares públicos. En este artículo argumentamos el lugar donde se ejecuta una medida invasiva de la privacidad es menos decisivo, a la hora de establecer la intrusividad de tal disposición con respecto a la esencia del derecho a la privacidad, que el secretismo de tal medida.*

Palabras clave: *GPS, leyes de los Derechos Humanos, privacidad, secreto, tecnologías de detección.*

Autor

Mathias Vermeulen es investigador de la Facultad de Derecho del Instituto Universitario Europeo (EUI) en Florencia y colaborador a tiempo parcial en el Grupo de Investigación en Derecho, Ciencia, Tecnología y Sociedad (LST) en la *Vrije Universiteit Brussel* (VUB).

1. Introducción

Según la Comisión Europea, el término "tecnología de detección" se puede referir a casi cualquier cosa "*usada para detectar algo en un contexto de seguridad o protección, enfocado al cumplimiento de la ley, a las fronteras o a las autoridades de seguridad*"[1]. Recientemente el Coordinador Europeo de lucha contra el terrorismo destacó la importancia de las tecnologías de detección que permitió la investigación de servicios de tecnologías de la información (TI), la interceptación de telecomunicaciones y el uso de sistemas de seguimiento (u otros equipos de grabación) puestos debajo o dentro de vehículos en movimiento en el territorio de varios Estados miembros. Según el Coordinador Europeo de lucha contra el terrorismo, el "fenómeno del terrorismo" es ahora "tan especializado" que "*a menudo sólo puede ser descubierto con técnicas de investigación relativamente sofisticadas*"[2].

El mensaje de que las nuevas tecnologías son necesarias para contrarrestar las nuevas amenazas del terrorismo no es nuevo. Hace treinta años que la Comisión Europea de Derechos Humanos (CEDH) ya manifestaba lo siguiente:

Las sociedades democráticas hoy en día se encuentran amenazadas por formas sofisticadas de espionaje y terrorismo, por lo que el Estado debe ser capaz, en orden a contrarrestar eficazmente estas amenazas, de llevar a cabo la observación secreta de los elementos subversivos que operen dentro de su jurisdicción[3].

Poco parece haber cambiado en los últimos 30 años: la vigilancia mediante el uso de nuevas tecnologías continúa siendo vista como una herramienta vital para evitar los ataques terroristas.

Al mismo tiempo, estas tecnologías de control amenazan o violan el derecho a la privacidad. El Tribunal Europeo de los Derechos Humanos ha desarrollado un conjunto de garantías mínimas con respecto al uso de las tecnologías de observación específicas que son usadas de forma encubierta para interceptar comunicaciones, pero recientemente dictaminó, en el caso Uzun v. Alemania[4], que esas salvaguardias no son aplicables a la vigilancia oculta con dispositivos GPS que realicen un seguimiento de los movimientos de un sospechoso.

Nosotros discrepamos de esa posición y sostenemos que el factor principal determinante de la gravedad de la interferencia, de acuerdo con la esencia del derecho a la privacidad, no es si una tecnología detecta o no localizaciones, movimientos o expresiones de las personas, sino si lo hace o no secretamente.

2. El núcleo del derecho a la privacidad

Determinar qué elementos del derecho a la privacidad representan el ''núcleo" de este derecho o, en otras palabras, son "esenciales" no es una cuestión puramente teórica; debería afectar al desarrollo, la implementación y el uso de las tecnologías específicas de investigación. En "X e Y contra Holanda", la Corte, por ejemplo, ha indicado que la naturaleza de la obligación del Estadode proteger un derecho dependerá del aspecto particular de la vida privada que está en cuestión. En un caso donde "aspectos básicos de la vida privada están en juego" el margen de apreciación es pequeño[5]. Abordar cuestiones relacionadas con la protección de datos personales no será suficiente para determinar los límites del uso de tecnologías de detección. En este contexto, el derecho es predominantemente procesal: informa del derecho a la intimidad y proporciona parámetros importantes de control sobre algunos aspectos de la vida privada de una persona[6].

El núcleo inviolable de un derecho es una subcategoría de un derecho humano que se aplica de manera absoluta, para que dentro de su ámbito de aplicación, este núcleo determine el resultado del caso, independientemente de que se hagan otros argumentos jurídicos cualesquiera. Un derecho puede llevar más de un núcleo, es decir, contar con más normas específicas para clasificarse como una regla[7].

En el caso de la privacidad, por ejemplo, se podría argumentar que existen al menos dos áreas "centrales". La primera parte se refiere al núcleo "esencial" de "pura privacidad" y es similar a la dimensión de *forum internum* de la libertad de religión, que se refiere al ámbito interno y privado de la persona contra el cual no se justifica interferencia del Estado bajo ninguna circunstancia[8].

Asimismo, la dimensión de *forum internum* del derecho a la privacidad podría constituir el derecho de un individuo a su propia identidad o identidades, incluyendo el derecho a cambiarla o cambiarlas y a no divulgar estas identidades. Un aspecto concreto de este elemento de *forum internum* del derecho a la intimidad incluye la libertad de expresar los sentimientos más íntimos o la sexualidad.

En Alemania el *Bundesverfassungsgericht* (Tribunal Constitucional Federal) desarrolló este elemento del núcleo del derecho a la privacidad en un caso con respecto a la "vigilancia acústica". En este caso el Tribunal dictaminó que cada operación de seguimiento tiene que interrumpirse si hay indicios de que

> “El riesgo de la arbitrariedad en las intromisiones en el derecho a la privacidad es mayor cuando el poder ejecutivo se ejerce en secreto”

esta vigilancia afectará, entre otras cosas, a la expresión de los sentimientos más íntimos o a la sexualidad”[9].

La segunda parte del núcleo del derecho a la privacidad se centra en su valor social: su capacidad para proteger otros derechos humanos, incluyendo áreas clave por un lado y su función de activación para el disfrute de otros derechos por el otro. El derecho a la intimidad sirve como base para otras libertades fundamentales, como la libertad de expresión, la libertad religiosa, la libertad de asociación o la libertad de movimientos. Sin intimidad estas otras libertades no se desarrollarían y disfrutarían de manera efectiva[10].

Las intromisiones en la base de la privacidad conducen al infame “efecto inhibidor”, que es perjudicial para la democracia porque da como resultado una autocensura cuando se expresan creencias desviadas e inhibiciones al realizar acciones “no convencionales”. Las injerencias en la base de lo privado amenazan no sólo estas actividades, sino también (en palabras de Jeffrey Rosen) *apagan gradualmente la fuerza de nuestras aspiraciones hacia ello*[11] .

El derecho a la intimidad en este contexto funciona principalmente como un límite al poder del Estado. Visto desde esta perspectiva, puede decirse que el lugar donde se lleva a cabo una orden que viola la privacidad es menos determinante a la hora de establecer la intrusividad de esta disposición en el corazón del derecho a esta privacidad que el secreto de tal medida.

El diseño de Jeremy Bentham para un panóptico mostró esto ya en el año 1791[12]: ser conscientes de la posibilidad de ser vigilados es justamente tan inhibidor como la vigilancia real. O, como Solove destaca más recientemente: “*de hecho, puede haber un efecto amedrentador aún mayor cuando las personas son generalmente conscientes de la posibilidad de ser espiadas, pero nunca están seguras de que están siendo observadas en un momento dado*”[13].

3. Desafíos planteados por las intromisiones secretas en el derecho a la privacidad

El Tribunal Europeo de los Derechos Humanos ha puesto de relieve la amenaza de las injerencias secretas en el derecho a la vida privada en su jurisprudencia en el artículo 8[14].

Hay varias razones para esto. El riesgo de la arbitrariedad en las intromisiones en el derecho a la privacidad es mayor cuando el poder ejecutivo se ejerce en secreto[15]. Ya que las medidas ocultas se establecen sin el conocimiento de la persona que se ha puesto bajo vigilancia, la búsqueda de un remedio eficaz contra esta interferencia se hace más difícil o incluso imposible. A menudo el interesado tampoco puede tomar parte directa en cualquier procedimiento de revisión de la intromisión[16].

La Corte ha señalado que esto tiene un impacto más allá de la persona. En ese contexto, “*la sospecha generalizada y la preocupación entre el público en general de que los poderes abusan de la vigilancia oculta*” no estarían injustificadas según el Tribunal[17]. Teniendo en cuenta el riesgo intrínseco de abuso en “cualquier sistema de vigilancia encubierta”, la Corte ha afirmado que cualquier sistema de este tipo “*debe basarse en una ley que sea particularmente precisa, especialmente cuando la tecnología disponible se está haciendo cada vez más sofisticada*”[18].

Parece indiscutible pues que el único uso secreto legítimo de las tecnologías de seguimiento se puede dar en el contexto de la investigación o prevención de un delito grave.

El Tribunal Europeo de los Derechos Humanos ha señalado, por ejemplo, que las escuchas telefónicas encubiertas constituyen una “intromisión muy grave” en los derechos de una persona y que “*sólo motivos muy serios, basados en una sospecha razonable de que la persona está involucrada en actividades delictivas graves, deben tomarse en cuenta como base para autorizarlas*”[19].

Ha indicado, además, que la vigilancia secreta de los ciudadanos sólo es permisible en la medida en que sea estrictamente necesaria para salvaguardar las instituciones democráticas, porque un sistema de vigilancia secreta para proteger la seguridad nacional conlleva el riesgo de “*socavar o incluso destruir la democracia en lugar de defenderla*”[20].

El Tribunal Europeo de Derechos Humanos ha desarrollado un estricto conjunto de garantías mínimas que deben establecerse en ley con el fin de evitar los abusos de poder en casos de medidas secretas de vigilancia: la naturaleza de los delitos que pueden dar lugar a vigilancia; una definición de las categorías de personas que puedan verse sometidos a tal seguimiento; un límite en la duración del mismo; el procedimiento que debe seguirse para examinar, usar y almacenar los datos obtenidos; las precauciones que deberán tomarse al comunicar los datos a otras partes, y las circunstancias en que estos datos obtenidos serán suprimidos[21].

4. ¿Nuevas herramientas, nuevos desafíos? Rastreadores GPS

Mientras que el Tribunal Europeo de los Derechos Humanos ha desarrollado un conjunto de garantías mínimas con respecto al uso de las tecnologías de detección específicas que se utilizan en secreto para interceptar las comunicaciones, la Corte dijo recientemente que estas garantías mínimas concretas que deben ser establecidas como ley no son aplicables a la vigilancia secreta con un dispositivo GPS[22], porque el seguimiento secreto con un sistema de este tipo se considera menos intrusivo en la vida privada de una persona que, por ejemplo, las escuchas telefónicas[23]. La Corte ha dicho de la vigilancia vía GPS que:

“Por su propia naturaleza” debe distinguirse de “*otros métodos de seguimiento acústico o visual que, por regla general, son más susceptibles de interferir con el derecho de la persona al respeto a su vida privada, porque revelan más información sobre la conducta de una persona, sus opiniones o sus sentimientos*”[24].

El Tribunal dejó pasar aquí una oportunidad para afinar el derecho a la intimidad en el siglo XXI. La Corte no tuvo en cuenta aquí la importancia emergente del concepto de localización privada, que puede definirse como la capacidad de un individuo para moverse en espacios públicos con la expectativa de que en condiciones normales su ubicación no se registrará de forma sistemática ni secreta para su uso posterior[25]. En palabras de Beresford y Stajano, la privacidad en la ubicación es “*la capacidad para impedir que otras partes conozcan una localización actual o pasada*”[26]. Este concepto es cada vez más importante ya que los datos de ubicación de los GPS y de los teléfonos móviles permiten la localización de un individuo a una escala mucho mayor, lo que posibilita la correlación del comportamiento individual a objetos, a lugares y a otras personas[27].

Además de estas dos fuentes de datos tan importantes de localización (sistemas GPS y teléfonos móviles), existen asimismo otras técnicas con las cuales se puede obtener información de ubicaciones, incluyendo sistemas RFID (*Radio Frequency IDentification*) y las aplicaciones biométricas[28]. Todos estos datos pueden esbozar un cuadro del comportamiento de comunicación del usuario,

> “La Corte dijo recientemente que estas garantías mínimas concretas que deben ser establecidas como ley no son aplicables a la vigilancia secreta con un dispositivo GPS, porque el seguimiento secreto con un sistema de este tipo se considera menos intrusivo en la vida privada de una persona”

de sus acciones, paradero o movimientos, que pueden revelar detalles sobre los perfiles personales, relaciones y otros aspectos de la vida del individuo que normalmente no podrían ser observados por otras personas.

El seguimiento secreto de los datos de localización, “por su propia naturaleza”, no debe distinguirse de la vigilancia visual. El secreto de esta medida lo hace también potencialmente amenazante para el núcleo del derecho a lo privado. Dicha vigilancia, llevada a cabo durante un período prolongado de tiempo, es capaz de revelar tanta información sobre la conducta de una persona como una llamada telefónica interceptada, y la monitorización de estos movimientos tiene un efecto igualmente escalofriante sobre el disfrute de otros derechos.

El argumento anterior no impide a nadie sostener que la vigilancia secreta de expresiones personales como voz o texto sea una injerencia más grave en la base del derecho a la privacidad. Pero es lamentable que el Tribunal no decidiera aplicar las normas estrictas de Weber y Saravia en el uso de sistemas de rastreo GPS. El factor principal determinante de la gravedad de la intromisión en el corazón del derecho a lo privado no es si una tecnología descubre ubicaciones, movimientos o expresiones de personas, sino si lo hace de manera encubierta. La distinción entre la detección de movimientos y la de expresiones sería solamente un paso secundario.

5. Conclusión

Este artículo argumenta que las tecnologías de seguimiento que se utilizan de forma oculta constituyen la más grave interferencia con lo básico del derecho a la intimidad; la distinción entre el rastreo de movimientos (públicos) y de expresiones (privadas) ocurrirá sólo como un paso secundario para determinar la gravedad de esta intromisión. Este seguimiento encubierto de datos de ubicaciones no debería, por su naturaleza, distinguirse de la vigilancia visual; también puede revelar información confidencial y los tribunales, por lo tanto, deben otorgar más importancia a las garantías procesales que se añaden a esta última clase de vigilancia.

Notas

[1] COM (2006) 474, pág .19.
[2] Coordinador antiterrorista de la UE. Dimensión Judicial de la lucha contra el terrorismo: Recomendaciones para la acción, Doc 13318/1/10, de 28 de septiembre de 2010, pág. 3.
[3] Comisión Europea de los Derechos Humanos. Klass y otros contra República Federal de Alemania, solicitud Nº 5029/71, 1977, párr. 48.
[4] Tribunal Europeo de los Derechos Humanos. Uzun v. Germany. *Application no. 35623/05*. <http://ius.unibas.ch/fileadmin/user_upload/fe/file/EGMR_Uzun_v._Germany__2010_.pdf>.
[5] Comisión Europea de los Derechos Humanos. X e Y v. The Netherlands, sentencia de 26 de marzo de 1985, párrafos. 24-27.
[6] Para un más amplio debate véase: Paul De Hert, Serge Guthwirt. Data protection in the case law of Strasbourg and Luxemburg: Constitutionalism in action, en “Reinventing data protection”, Serge Gutwirth, Yves Poullet, Paul De Hert, J. Nouwt y C. De Terwangne (editores.) Springer Science, Dordrecht, 2009, pp. 3-44.
[7] Martin Scheinin. *Terrorism and the pull of ‘balancing’ in the name of security*. En Martin Scheinin (ed.), “*Law and Security - Facing the dilemmas*”. Martin Scheinin editor. EUI (Instituto Universitario Europeo), documento de trabajo de Derecho 2009/11, 2009, pág. 55.
[8] CCPR/C/21/Rev.1/Add.4, General Comment No. 22: *the right to freedom of thought, conscience and religion*, 30 de julio de 1993, párrafo 3.
[9] G. Hornung, C. Schnabel. Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention. Computer Law & Security Review 25, núm. 2 (2009): pág. 117.
[10] Martin Scheinin. Documento de las Naciones Unidas A/HRC/13/37. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 28 de diciembre de 2009, párrafo 33.
[11] Jeffrey Rosen. *The Naked Crowd: Reclaiming Security and Freedom in an anxious age*. Londres, Random House (2004), pág.36.
[12] El panóptico es un centro penitenciario imaginario diseñado por el filósofo Jeremy Bentham en 1791. El concepto de este diseño permite a un vigilante observar (*-opticón*) a todos (*pan-*) los prisioneros sin que éstos puedan saber si están siendo observados o no. <http://es.wikipedia.org/wiki/Pan%C3%B3ptico>.
[13] Daniel Solove. *A taxonomy of privacy*. Revista de Leyes de la Universidad de Pennsylvania 154, número 3 (enero de 2006): p. 495.
[14] Ver más recientemente: TEDH (Tribunal Europeo de los Derechos Humanos). Weber y Saravia contra Alemania, diligencia núm. 54934/00 (Decisión de Accesibilidad) (2006), párrafo 93; Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev contra Bulgaria, diligencia núm. 62540/00 (2007), párrafo 75; Liberty y Otros contra el Reino Unido, diligencia núm. 58243/00, (2008) párrafo 62; y Iordachi y otros contra Moldavia, diligencia núm. 25198/02, (2009), párrafo 39.
[15] TEDH y Bykov contra Rusia (diligencia núm. 4378/02),(2009) párrafo 78; Huvig contra Francia, diligencia núm. 11105/84, (1990) páginas 29-32.
[16] Véase también Comisión Europea de los Derechos Humanos. Klass y otros contra la República Federal de Alemania, diligencia núm. 5029/71. (1977), párrafo 52.
[17] Tribunal Europeo de los Derechos Humanos y Kennedy contra el Reino Unido (diligencia núm. 26839/05) (2010), párrafo 124.
[18] TEDH y Kopp contra Suiza, diligencia núm. 13/1997/797/1000,(1998) pág. 72; Weber y Saravia contra Alemania , diligencia núm. 54934/00 (Decisión de aceptación) (2006), párrafo 93.
[19] TEDH, Iordachi y otros contra Moldavia, diligencia núm. 25198/02 (2009), párrafo 51.
[20] Comisión Europea de los Derechos Humanos y Klass contra la República Federal de Alemania, diligencia núm. 5029/71 (1977), párrafo 49.
[21] TEDH, Weber y Saravia contra Alemania, diligencia núm. 54934/00 (Decisión de aceptación) (2006), párrafo 95.
[22] TEDH y Uzun contra Alemania, (diligencia núm. 35623/05) (2010), párrafo 66.
[23] Idem, párrafo 72. Id
[24] Idem, párrafo 52.
[25] Andrew J. Blumberg, Peter Eckersley. “*On Locational Privacy, and How to Avoid Losing it Forever*” (Electronic Frontier Foundation, agosto 2009), pág. 2.
[26] A.R.Beresford, F. Stajano. “*Location Privacy in Pervasive Computing*”. IEEE Pervasive Computing, 2(1), pp. 46-55.
[27] Ronald Leenes. Mind my step?, TILT, serie de documentos de trabajo sobre tecnología y derecho, número 011 (2009), pág. 6.
[28] Nouwt, ibid. nota 22, en 381.